(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 709 760 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.05.1996 Bulletin 1996/18

(51) Int. Cl.[6]: **G06F 1/00**, G06F 12/14

(21) Application number: **95116820.2**

(22) Date of filing: **25.10.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **27.10.1994 JP 264201/94**

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku Tokyo 100 (JP)

(72) Inventors:
- **Saito, Makoto**
  Tokyo (JP)
- **Momiki, Shunichi**
  Tokyo (JP)

(74) Representative: **Neidl-Stippler & Partner**
Rauchstrasse 2
D-81679 München (DE)

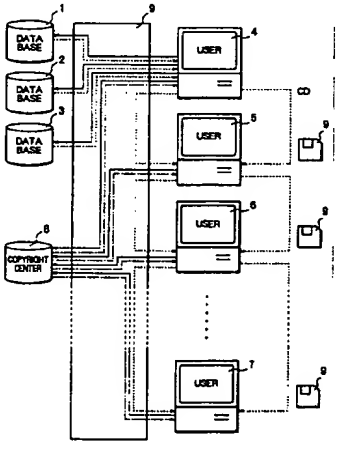
(54) Data copyright management system

(57) A system is provided which manages the copyright of a plurality of data in a database. A data copyright management system is provided in which a primary user edits data which he or she obtains and supplies edited data to a secondary user.

In a case where new data is produced by editing a plurality of encrypted data obtained from the database, and is encrypted for distribution to another person, crypt keys for a plurality of data as raw material and an edition program which is an editing process with a digital signature are used as a use permit key. When a user who receives the edited and encrypted data requests use of the data by presenting the digital signature to a copyright management center, the copyright management center identifies the editor by the digital signature, and provides the user requiring use of data with the crypt key for use only when the editor is identified to be the valid user of the edited data. The system comprises a database and a key control center, and uses a primary copyright label, a first use permit key including a first crypt key, a second use permit key, a third crypt key, and a copyright management program. The primary user uses primary copyrighted data encrypted by using the first crypt key and supplied, by decrypting it with the first use permit key obtained from the key control center. The data is encrypted again by using the first use permit key when it is stored. The primary user edits the primary copyrighted data by obtaining a second use permit key from the key control center for editing the primary copyrighted data. The data being edited is encrypted and stored by using the second use permit key. At the completion of the editing, the primary user receives the third crypt key for secondary copyright as secondary exploitation right, encrypts the edited data with the third crypt key, and distributes it to a secondary user. The secondary user obtains the third crypt key and uses the edited data.

In another system, in a case where a new data is produced by editing a plurality of data obtained from the database, and encrypted for distribution to another person, crypt keys for a plurality of data as raw material and an edition program which is as an editing process with a digital signature are used as a use permit key. When a user who receives the edited and encrypted data requests use of the data by presenting the digital signature to a copyright management center, the copyright management center identifies the editor by the digital signature, and provides the user requiring data use with a crypt key for use only when the editor is identified to be the valid user of the edited data.

FIG. 1



EP 0 709 760 A2

Description

Field of the Invention

The present invention relates to a system for managing the copyright for the use of digital data, that is, the display, storage, copying, edition, and transmission of such data, which is particularly applicable to a multimedia system.

Background of the Invention

As more and more information is available, database systems wherein many computers, which independently stored various data, are connected via communication lines to use the data mutually are becoming increasingly popular.

Such database systems has been so far possible to process only coded information containing a small amount of information which can be processed by conventional computers and at the most monochrome binary data such as facsimile information, and failing to handle natural and moving pictures that include a substantially large amount of information.

Digital processing techniques for various electric signals are being developed, and efforts are being made to apply such techniques to those dynamic picture signals other than binary data which were processed as analog signals.

Since the digitalization of picture signals enables picture signals such as television signals to be handled by computers, people are viewing as a promising technique a "multimedia system" that can deal with both various data that can be processed by computers and picture data that is digitalized picture signals.

Since picture data contains a significantly larger amount of information than character data or audio data, it cannot be stored, transmitted, or subjected to various processings by computers in its original form.

Attempts have thus been made to compression/expansion picture data, and some picture data compression/expansion standards have been prepared. These standards include the following common standards: the Joint Photographic Image Coding Experts Group (JPEG) standards for still pictures, the H. 261 standards for video conferences, the Moving Picture Image Coding Experts Group 1 (MPEG1) standards for picture storage, and the MPEG2 standards for both existing television broadcasting and future high-precision television broadcasting.

These techniques have enabled digital picture data to be processed in real time.

Since analog data, which is conventionally popular, is degraded each time it is stored, copied, edited, and transmitted, little notice has been taken of the control of the copyright associated with these operations. Digital data, however, is not degraded after repeated storage, copying, edition, and transmission, such control is significant.

There has been no adequate method for controlling the copyright for digital data; the copyright is managed based on the copyright law or relevant contracts. The copyright law simply establishes a compensation system for digital recording equipment.

A database not only has its contents referenced but is also used to effectively use data obtained through storing, copying, and edition and transfer edited data to a different user through copying or transmission, or to receive and register new data to a databasea.

Although conventional databases have dealt with only character data, databases in multimedia system contain audio and picture data that is inherently analog, in addition to character data.

Under these circumstances, the control of the copyright for data in databases is very important, but no copyright management means that is particularly applicable to secondary use such as copying, edition, and transmission has been completed.

The inventors have proposed in Japanese Patent Application 1994-46419 and Japanese Patent Application 1994-141004 a system for managing the copyright by forcing the user to acquire a permit key from the key control center through a public telephone line, and in Japanese Patent Application 1994-132916 an apparatus for this purpose.

By improving these inventions, the inventors have also proposed in Japanese Patent Application 1994-64889 a copyright management method applicable to both the primary use of a database system such as the display (including audio output) and storage of digital data and the secondary use such as copying, edition, and transmission, including the realtime transmission of digital picture.

To manage the copyright for a database system, this database copyright management method uses in the database system a program and copyright information required to manage the copyright in addition to a key for permitting to use which is transmitted to the user.

The copyright management program watches and manages to prevent users from using other than the conditions of users' request or permission.

The inventors have also proposed in Japanese Patent Application 1994-237673 a database copyright management system for specifically implementing the database copyright management method proposed in Japanese Patent Application 1994-64889 described above.

The system proposed in Japanese Patent Application 1994-237673 comprises a key management center that manages a crypt key K and a copyright management center that manages the database copyright. According to this system, all the data delivered from a database is encrypted by a first crypt key K1, and a primary user who wishes to uses data directly from the database requests the key management center for the key K corresponding to the specific usage by presenting information I1 on the user to the center. In response to the primary usage request from the primary user, the key

management center transfers the information I1 on the user to the copyright management center. On receiving the information I1, the copyright management center transfers this information I1 with a copyright management program Pc to the key control center. On receiving the copyright management program Pc, the key control center transfers the first crypt key K1 and a second crypt key K2 corresponding to the specific usage together with the copyright management program Pc to the primary user via a communication network. On receiving the first crypt key K1, the primary user uses this key to decrypt the data. The user subsequently uses the second crypt key K2 to encrypt and decrypt data when storing, copying or transmitting the data.

In cryptographic techniques, the use of the crypt key K to encrypt a plaintext M to obtain a cryptogram C is expressed as:

C = E (K, M)

while the use of the crypt key K to decrypt the cryptogram C to obtain the plaintext M is expressed as:

M = D (K, C).

These expressions are used hereafter in this specification.

If data is copied to an external record medium or transmitted without being stored, the first and second crypt keys K1 and K2 are disued. If the primary user wishes to use the data again, the first and second crypt keys K1 and K2 are re-delivered to the user from the copyright management center. The re-delivery of the second crypt key K2 indicates a confirmation that the data has been copied or transferred to a secondary user, and this is recorded in the copyright management center.

In requesting a secondary usage to the copyright management center, the secondary user presents the information I1 on the primary user and information I0 on the original copyright to the copyright management center.

The copyright management center transmits to the secondary user a permit key Kp corresponding to the specific usage with a second crypt key K2 (viewing permit key), a third crypt key K3 (a permit key corresponding to the specific usage), and the copyright management program Pc which have been encrypted.

Typical means used for encrypting data include secret-key cryptosystem and public-key cryptosystem.

The secret-key cryptosystem uses the same secret crypt key Ks for both encryption and decryption:

CmKs = E (Ks, M)

M = D (Ks, Cmks).

In the public-key crypt system, a key for encryption is open as a public-key, while a key for decryption is not open and is called a private-key. To use this cryptosystem, a n information provider encrypts using the public-key Kb for a receiver

Cmkb = E(Kb, M),

while the receiver receiving the encrypted data decrypts it using the private-key Kv that is not open

M = D (Kv, Cmkb).

In the application submitted simultaneously with this application, the inventors have proposed an invention that employs a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2S, and a second private-key Kv2 corresponding to the second public-key Kb2 which are prepared by the user, and a first secret-key Ks1 and a second secret-key Ks2 prepared by the database. The database uses the first secret-key Ks1 to encrypt data M

Cmks1 = E (Ks1, M)

and further encrypts the firstsecret-keys Ks1 by the first public-key Kb1

Cks1kb1 = E (Kb1, Ks1)

and encrypts the second secret-key Ks2 by the second public-key Kb2

Cks2kb2 = E (Kb2, Ks2);

the database then transmits these encrypted data Cmks1 and the first and the second secret-keys CKs1 and Cks2kb2 to the user;

the user decrypts the first secret-key Cks1kb1 using the first private-key

Kv1

Ks1 = D (Kv1, Cks1kb1),

and decrypts the encrypted data Cmks1 to use by decrypted first secret-key Ks1

M = D (Ks1, Cmks1),

and the encrypted second secret-key Cks2kb2 by the second private-key Kv2

Ks2 = D (Kv2, Cks2kb2);

and decrypted second secret-key Ks2 is used for data storage/copy/transfaer after data decryption.

SUMMARY OF THE INVENTION

The database copyright management system proposed in Japanese Patent Application 1994-237673 assumes that a single data or database is used in the system, and not that that a plurality of data or databases are edited to produce new data.

The inventors thus proposes in this application a data copyright management system assuming that a plurality of data or databases are edited to produce new data.

If a plurality of encrypted data obtained from one or more databases are edited to produce and encrypt new data and if the encrypted data is then supplied to a different user, this system employs as a use permit key, both a crypt key for each of the plurality of data that are a source material and data of an edition program used as an edition process with a digital signature.

Upon receiving edited and encrypted data, a different user requests the use of the data by presenting the data with the digital signature to the copyright management center. The copyright management center then identifies from the digital signature the person who has edited the data, and supplies a key for using the data to the user when requested the use only if it has confirmed that the person who has edited the data is a valid user of this data.

In another system, a primary user who requires to use original data encrypted and supplied using the first crypt key requests the key control center to sent primary use permit key. The key control center distributes the primary use permit key to the primary user and charges therefor.

The primary user decrypts encrypted data using the first crypt key included in the first use permit key to use the data. When decrypted data is stored in the primary user device, it is encrypted again using the first use permit key.

The primary user who requires to edit data requests the key control center for distributing secondary use permit key for data edition. The key control center distributes the secondary use permit key to the primary users. The primary user who receives the secondary use permit key produces the copies of primary copyrighted data, edit copied data, encrypts decrypted secondary data during edition by the second crypt key included in the secondary use permit key.

Finally edited data is encrypted using the third crypt key and stored in the primary user device. The primary user registers the third crypt key into the key control center in order to execute the secondary copyright as secondary exploitation right with reference to the data edition for the secondary copyrighted data, encrypts the secondary data using the third crypt key and supplies the secondary user with such data by copying it to an external medium or by transferring it via a network system.

The secondary user who requires encrypted secondary data requests the key control center for distributing the third crypt key. The key control center distributes the third crypt key to the secondary user.

The secondary user who receives the second crypt key decrypts encrypted secondary data using the second crypt key to use it.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of an embodiment of a data copyright management system according to this invention.

Figure 2 is an example illustrating of producing new copyrighted data using a plurality of copyrighted data as objects.

Figure 3 is an outlined block diagram of another embodiment of data copyright management system according to this invention.

Figure 4 is an example illustrating of producing new copyrighted data using a plurality of copyrighted data as objects.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

An embodiment of this invention is described with reference to the drawings.

Figure 1 shows a block diagram of a data copyright management system according to this invention. The data stored in the database in this system is not encrypted.

In addition to databases, the embodiment in Japanese Patent Application 1994-237673 uses satellite broadcasting or a storage medium as a means for supplying data. In the embodiment shown in this application, however, only databases are shown as a means for supplying data for the convenience of explanation. Of course, however, this invention is applicable to the use of satellite, terrestorial wave or CATV broadcasting that is free due to advertisement and the like and this does not require encryption, or a record medium as well as databases as a means for supplying data.

If a primary user copies data obtained and then supplies it to a secondary user, the data does not involve the copyright of the primary user because no modifications have not been made to the data. If, however, the primary user produces new data based on the data obtained or using a means for combining the original data with other data, the new data involves a secondary exploitation for the primary user.

Similarly, if the secondary user produces new data based on the data obtained from the primary user or using a means for combining the original data with other data, the new data involves a secondary copyright as secondary exploitation right for the secondary user.

In the embodiment shown in the figure, reference numerals 1, 2, and 3 designate databases that store text data or binary, audio, and/or picture data constituting computer graphics screens or programs, the data which is not encrypted; 9 is a communication line such as a public telephone line provided by a communication enterprise or a CATV line provided by a cable television enterprise; 4 is a primary user terminal; 5 is a secondary user terminal; 6 is a tertiary user terminal; and 7 is an n-th user terminal device. In addition, reference numeral 8 designates a copyright management center for managing the data copyright.

The databases 1, 2, and 3, copyright management center 8, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-th user terminal 7 are connected to a communication line 9.

In this figure, encrypted data is transmitted via the path shown by a broken line, requests are transmitted from the user terminal 4, 5, 6, or 7 to the database 1, 2, or 3 and the copyright management center 8 via the path shown by a solid line, the permit key, copyright management program, and crypt key corresponding to a specific usage are transmitted from the database 1, 2, or 3 and the copyright management center 8 to the user terminal 4, 5, 6, or 7 via the path shown by an one-dot chain line.

This embodiment employs a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2, and a second private-key Kv2 corresponding to the second public-key Kb2 which are prepared by the user, and a first secret-key Ks1 and a second secret-key Ks2 prepared by the database. The database uses the first secret-key Ks1 to encrypt data M

Cmks1 = E (Ks1, M)
and further encrypts the first secret-key Ks1 by the first public-key Kb1
Cks1kb1 = E (Kb1, Ks1)
and the second secret-key Ks2 by the second public-key Kb2
CKs2kb2 = E (Kb2, Ks2).
The database then transmits these encrypted data Cmks1 and the first and the second secret-keys Cks1kb1 and Kcs2kb2 to the user.

The user decrypts the encrypted first secret-key Cks1kb1 using the first private-key Kv1
Ks1 = D (Kv1, CKs1kb1),
and decrypts the encrypted data Cmks1 by the decrypted first secret-key Ks1
M = D (Ks1, Cmks1)
and use it. And further, the user decrypts encrypted second secret-key Cks2kb2 by the second private-key Kv2
Ks2 = D (Kv2, Cks2kb2),
which is subsequently used as a crypt key for storing, copying, or transmitting data.

If a primary user 4 copies data obtained and then supplies it to a secondary user 5, the data does not involve the copyright of the primary user 4 because no modifications have not been made to the data. If, however, the primary user 4 produces new data based on the data obtained or using a means for combining the original data with other data, the new data involves a secondary exploitation right for the primary user 4, and the primary user 4 has the original copyright for this secondary work.

Similarly, if the secondary user 5 produces new data based on the data obtained from the primary user 4 or combining with other data, the new data involves a secondary exploitation right for the secondary user 5, and the secondary user 5 has the original copyright of this secondary work.

The databases 1, 2, and 3 store text data or binary, digital audio, or digital picture data constituting computer graphics screens or programs, the data which is not encrypted. This data is encrypted and supplied to the user terminal 4 via the communication line 8 during a data reading operation in response to a request from the primary user terminal 4.

The data copyright obtained from the database is managed by the method described in Japanese Patent Application 1994-237673 or in the application submitted simultaneously with this application.

A summary of the applications proposed by the inventors of this invention are shown below.

Both the secret-key and public-key cryptosystems are adopted as crypt methods. Although the use of the public-key cryptosystem in the encryption of data improves the security of encrypted data, the encryption of data containing a large amount of information using the same system requires a significantly long time for decryption and is not practical.

The amount of information contained in crypt keys, however, is not so large as that in data because such keys must be operated by human beings.

This copyright management system employs a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2, and a second private-key Kv2 corresponding to the second public-key Kb2 which are prepared by the user, and a first and a second secret-keys Ks1, Ks2 prepared by the database.

The database uses the first secret-key Ks1 to encrypt data M
Cmks1 = E (Ks1, M)
and further encrypts the first secret-key Ks1 using the first public-key Kb1
Cks1kb1 = E (Kb1, Ks1)
and the second secret-key Ks2 using the second public-key Kb2
Cks2Kb2 = E (Kb2, Ks2).
The database then transmits these encypted data and first and second secret-keys Cks1kb1, Cks2kb2 to the user.

The user decrypts the encrypted first secret-key Cks1kb1 using the first private-key Kv1
Ks1 = D (Kv1, Cks1kb1),
and decrypts the encrypted data Cmks1 using the decrypted first secret-key Ks1
M = D (Ks1, Cmks1)
to use it, and decrypts the encrypted second secret-key Cks2kb2 by the second private-key Kv2 which is to be used in subsequent storing, copying or transmitting decrypted data.

The edition of a plurality of data to produce new data is described with reference to Figure 2.

As shown in this figure, the primary user 4 extracts parts M4, M5 and M6 constituting data from a plurality of data M1, M2 and M3 obtained from one or more databases, and produces new data M7 from these parts M4, M5 and M6.

The primary user 4 supplies the new data M7 to the secondary user 5; the new data M7 involves a secondary coyright associated with the edition of original data M1, M2 and M3 as well as the original copyright for the original data M1, M2 and M3 from which the parts M4, M5 and M6 produces new data M7.

The original data M1, M2 and M3 are encrypted using the second secret-key Ks2 supplied with each of data M1, M2 and M3 when used for operation other than display; i.e., storage, edition, copying or transmission:
Cm1ks2 = E (Ks2, M1)
Cm2ks2 = E (Ks2, M2)
Cm3ks2 = E (Ks2, M3).
The data M4, M5 and M6, parts of original data are also encrypted using the second secret-key Ks2 supplied with each data when used for operation other than display:
Cm4ks2 = E (Ks2, M1)
Cm5ks2 = E (Ks2, M2)
Cm6ks2 = E (Ks2, M3).

The new data comprises the original data and the process that the data has been edited.

In the computer technology, the edition of data is represented by original data and an edition process for it. Furthermore, the original data and edition process can be represented by a computer program and the data written in the computer program. The program and data that have been an entire unit are referred to as "object", and the computer processing about objects is called an object-oriented technology, which has recently become most popular among the computer technologies.

The technique for producing new data from a plurality of data parts is called a frame work or scenario; the "Object Linking and Embedding" (OLE) program from Microsoft Corp. and "OpenDoc" from Apple Computer Inc. are typical examples.

This invention treats as objects the relationship between original data parts and a frame work or scenario constituting an edition process, in addition to the original data parts.

The primary user 4 who has edited the data provides a digital signature for edition program Pe using first Private-key

Spe = D (Kv1, Pe)

and supplies encrypted original data parts Cm4ks2, Cm5ks2 and Cm6ks2 to secondary user 5 together with the edition program Pe with digital signature.

Upon receipt of the encrypted original data parts Cm4ks2, Cm5ks2 and Cm6ks2, and the edition program Pe, the secondary user 5 requests second secret-key Ks2 for decryption of the encrypted original data parts Cm4ks2, Cm5ks2 and Cm6ks2 to the copyright management center 8, by presenting the edition program Pe with digital signature.

The data copyright management center 8 identifies the primary user 4 from the presented digital signature in the edition program Pe, using first public-key Kb1

Pe = E (Kb1, Spe),

and determines if the primary user 4 is a valid user to use the original data to which the second secret-key Ks2 that has been requested corresponds. If the primary user 4 is a valid user, the cemter transmits the second secret-key Ks2 to the secondary user 5. Otherwise, it does not transmit the second secret-key Ks2 to the secondary user 5.

The digital signature Spe presented to the copyright management center 8 is registered in the center as a valid procedure for authorizing secondary copyright owner.

This system may limit appropriate n-order usage according to determination in practice by the database or original copyright owner, not permanetly repated usage from primary use till n-order use, and may make data which has been used certain-order be registered as next original data.

Another embodiment is described by referring to Figure 3.

This system uses primary use permit key K1 including first secret-key Ks1, secondary use permit key K2 including second secret-key Ks2, third secret-key Ks3, plaintext original copyright label Lc1 and plaintext copyright management program Pc.

The data copyright management system shown in Figure 3 comprises database 11, key control center 12, users 13, 13, 13 ... and the network 14 that connects these therewith mutually. Database 11 receives data from information providers (IP) 15, 15, 15.... However, in some cases, data is supplied directly to users 13 from information providers 16, 16, 16 ... via network 14 without intervening database 11.

The data used in this invention is the object comprising combined program and data.

Data is supplied from information providers 15, 15, 15 ... to database 11 and to primary users 13. However, in some cases, data is supplied from information providers 16, 16, 16 ... via network 14 or via information record medium 17 such as CD-ROM or the like directly to primary users 13 without intervening database 11.

The solid line, broken line and one-dot chain line in this figure show the path for data and requests for crypt keys, path of encrypted data and path of encrypt keys, respectively.

Primary users 13 are not merely users but can be information providers 15 or 16 that provide new data (secondary copyrighted data) by combining or revising obtained plural original data.

In the data copyright management system comprising in this way according to this invention, the original data provided by each of information providers 15 and 16 has been encrypted to protect the copyright. Therefore, the use of the encrypted original data obtained by users 13 needs decryption. All of the crypt keys for this decryption are deposited to key control center 12 to be controlled by this center.

Each of information providers 15 and 16 can adopt freely any cryptosystem. However, the cryptosystem described later and used after secondary utilization of ddata is limited to oen adopted by key control center 12.

The data obtained from databases are normally used through personal computers. The operating system used for this purpose requires incorporated functions for ensuring security control. Copyright management program is used to control crypt keys. As it is necessary to store this copyright management program and the crypt keys received from key control center 12, for example, a key card which is virtually implemented as hardware in unique board or PC card, or as software in the memory or HDD is used for the storage area.

Irrespective of whether key control center 12 is actually used or merely registered, it stores crypt key to protect the copyright of data works and to charge for using the copyright, and controls crypt key by establishing the correspondence between stored crypt key and copyright labels.

In this system, plaintext original data M0 is encrypted by 1first secret-key Ks1

Cm0ks1 = E (Ks1, M0),

and is provided to primary users 13 from information providers 15 via database 11 and network 14, or from infor-

mation provider 16 via network 14, or via information record medium 17 such as CD-ROM, together with original copyright label Lc1.

Original plaintext copyright label Lc0 is attached to encrypted original data Cm0ks1 provided for primary users 13, and which is used for obtaining primary use permit keys, etc. Namely, encrypted original data Cm0ks1 includes plaintext original copyright label Lc0 and encrypted original data Cm0ks1. The name of application programs in use, outlined explanation, fees and charging method are entered into plaintext original copyright label Lc0 in addition to general information including the name of original creator, title name and createed date. The number of use permit keys is also entered if necessary. Digital signature by original creator added to plaintext original copyright label Lc0 prevents false copyright claiming.

Primary users 13 who require use of encrypted original data Cm0ks1 request key control center 12 via network 14 for distributing primary use permit keys K1 indicating original copyright label Lc1.

Key control center 12 that has identified primary use permit keys to be distributed, by original copyright label Lc1 indicated, is key K1, distributes this identified key to primary users 13 via network system 14. Upon receip of distributed primary use permit key k1, the devicess of primary userss 13 are turned to the mode of copyright management, and the use of primary copyrighted data becomes available for primary users 13. As the first secret-key Ks1 is included in primary use permit key k1, it is not recognized by primary users 13.

On the other hand, key control center 12 charges as well as grasps the use condition of copyrighted data and of the database used by primary users 13.

Primary users 13 decrypt encrypted primary copyrighted data Cm0ks1 using first secret-key Ks1 included in primary use permit key K1

M0 = D (Ks1, Cm0ks1),

and use it.

When decrypted original data M0 is stored in primary users 13 devices, it is encrypted again by first secret-key Ks1

Cm0ks1 = E (Ks1, M0)

and encrypted original data Cm0ks1 is stored.

For repeated use of encrypted original data Cm0ks1, repeated decryption and encryption are carried out using first secret-key Ks1.

Primary users 13 who require to edit original copyrighted data M0 request key control center 12 for distributing secondary use permit key K2 via network 14.

Key control center 12 requested for distributing secondary use permit key K2 provides primary users 13 with secondary use permit key k2 via network 14.

Primary users 13 that have received secondary use permit key K2 edit original data M0 and obtain halfway edited data M0'.

When halfway edited data M0' is stored in users 13 devices, it is encrypted by second secret-key Ks2

Cm0'ks2 = E (Ks2, M0').

When the edition is finally completed, primary users 13 prepare third secret-key Ks3 in order to execute the secondary copyright with reference to the data edition concerning final editorial data M1, and register third secret-key Ks3 into key control center 12. The key control center 12 also may prepare third secret-key Ks3 and distribute it in response to the request from primary users 13.

When primary users 13 copy editorial data M1 into external reecord medium 18 or transfer it via network 14, they encrypt editorial data using third secret-key Ks3

Cm1ks3 = E (Ks3, M1)

and provide it for secondary users 19.

Secondary users 19 who require to use provided encrypted editorial data Cm1ks3 request key control center 12 for distributing third secret-key Ks3 via network 14.

Key control center 12 that has received the request for distributing third secret-keys Ks3 from secondary users 19 distributes third secret-key Ks3 to secondary users 19 via network 14.

Secondary users 19 who have received third secret-keys Ks3 decrypt encrypted editorial data Cm1ks3 using third secret-key Ks3

M1 = D (Ks3, Cm1ks3)

and use it.

When using encrypted data Cm1ks3 again, decryption and encryption are carried out using third secret-key Ks3 also in this case.

This section describes the restrictions applicable to the primary use carried out by copyright management program Pc.

Similarly to the invention described in prior Patent Application 1994-64889, the usage of the data obtained and decrypted according to the data copyright management system according to the invention is limited to normal form of use, namely, direct use of data and the output including the printing of usage results. Copying into external reecord medium, edition and transfer via network system, and, in principle, data storage inside devices are impossible. On the other hand, the storage of encrypted data is possible.

It goes without saying that it is possible to display, print, store, copy, edit and transfer the data of which copyright has not been claimed with reference to the application programs in use.

Encrypted original data Cm0ks1 that primary users 13 have obtained from external information providers 15 or 16 directly or via database 11 is combined with original copyright label Lc0 and stored in storage such as the hard disk driveor non-volatile memory inside the primary users 13 terminals.

Primary users 13 who require primary use of encrypted original data Cm0ks1 stored in memory identify the application environment of the program used by original data M0, referring to plaintext original copyright label Lc1.

When the original data M0 is determined to use possible as a result, and primary users 13 indicate to the

copyright management program Pc of using this original data M0, the copyright management program Pc activates application programs used by original data M0 and then, encrypted original data Cm0ks1 is read from storage into the volatile memory in the devices.

On the other hand, primary copyright label Lc1 is sent to key control center 12. When primary use permit key K1 is provided pursuant to the above processing flow, encrypted original data Cm0ks1 is decrypted using the first secret-key Ks1 included in primary use permit key K1

M0 = D (Ks1, Cm0ks1),

and its use becomes possible by means of the activated application program.

In the case original data M0 that has been decrypted in the volatile memory of primary users 13 terminals is to be stored in storage, it is encrypted using first secret-key Ks1

Cm0ks1 = D (Ks1, M0).

This storing includes the produce and storage of temporary file for data security.

When using again re-encrypted data Cm0ks1, repeated decryption/encryption are carried out using first secret-key Ks1.

In use of primary use permit key K1, it is possible to display and print decrypted original data M0 and store encrypted original data Cm0ks1 by copyright management program Pc. However, other form of usage; namely, store, edit, copy of decrypted original data M0, copy into external record medium and transfer it to other devices, and also copying encrypted original data Cm0ks1 into external record medium and transferring it to other devices are prohibited.

Therefore, it is prohibited to perform cut and paste from a part of original data M0 to other general data D, and to cut a part of general data D and paste it to original data M0 by means of copyright management program Pc.

It is exceptionally possible to store original data M0 in storage if it is with encrypted by first secret-key Ks1. However, storage is prohibited if any edition has been performed.

Copyright control program Pc distinguishes the original data M0 from the general data D of claiming no copyright, and judge whether original data M0 has been edited or not.

The above determination is carried out by examining the look-up table in which file attribute is written, comprising computer file together with file body. In this look-up table, in addition to the file size and produced date, a flag is written to show the copyright has been claimed. By examining these items, it is possible to judge whether the copyright has been claimed and whether the file has been edited.

Original data M0 is combined with original copyright label Lc1 as encrypted original data Cm0ks1 when it is stored in a storage. When it is decrypted and read into volatile memory, decrypted original data M0 and original copyright label Lc1 are separated by copyright management program Pc, and the separated copyright label Lc1 is controlled by copyright management program Pc.

Copyright management program Pc watches which application program is used for original data M0, and prohibits to cut and paste original data M0 on general data D and to cut and paste general data D on original data M0.

This section describes the restrictions applied to data edition by copyright management program Pc.

The primary users 13 who desire to edit original data M0 after primary usage, inform key control center 12 of the execution of original data M0 edition via network 14, and request key control center 12 for distributing secondary use permit key K2 for original data M0 edition.

Key control center 12 that has been requested for distributing secondary use permit key K2 distributes the key K2 to primary users 13 via network system 14.

By this, the primary users 13 terminal are changed to edit mode, and original data M0 edition by primary users 13 becomes possible.

After decrypting encrypted original data Cm0ks1 using first secret-key Ks1, primary users 13 display and edit data. In this case, original data M0 is copied at the beginning to protect it, and then, edition is applied to editorial data M0' obtained by this copying.

When this editorial data M0' or data M0" on the way of edition is stored in the storage inside the primary users 13 terminals, they are encrypted by the second secret-key Ks2 included in secondary use permit key K2 for storage:

Cm0'ks2 = (Ks2, M0'), or

Cm0"ks2 = (Ks2, M0").

Encrypted original data M0 is stored in the storage without being edited. Therefore, it is possible to judge whether the file is edited or not by examining the look-up table, the file size and date of producing of data M0" on the way of edition or edited data M1.

Plural primary edited data M11, M12, M13 ... are produced by data edition. The secondary copyright of primary users 13 as secondary exploitation right arises in these primary edited data M11, M12, M13 .... These primary edited data M11, M12, M13 are uncrypted when they are in the volatile memory of the primary users' terminals. However, when they are stored in a storage, they are encrypted using second secret-key Ks2

$$Cm11ks2 = E\ (Ks2,\ M11)$$

$$Cm12ks2 = E\ (Ks2,\ M12)$$

$$Cm13ks2 = E\ (Ks2,\ M13)$$

For the purpose of practice secondary copyright with reference to these primarily edited data M11, M12, M13 ..., primary users 13 request key control center 12 via network 14 for distributing third secret-key Ks3. In response to the request, key control center 12 distributes third secret-key Ks3 to primary users 13.

Primary users 13 who have received third secret-key s Ks3 encrypt plaintext or decrypted primarily edited data M11, M12, M13 ... using third secret-key

$$Ks3Cm11ks3 = E\ (Ks3,\ M11)$$

$$Cm12ks3 = E\ (Ks3,\ M12)$$

$$Cm13ks3 = E\ (Ks3,\ M13)$$

and encrypted primarily edited data Cm11ks3, Cm12ks3 and Cm13ks3 ... are stored in the storage inside primary users terminals.

When using these encrypted data Cm11ks3, Cm12ks3 and Cm13ks3 ..., decrypting and encrypting are carried out by third secret-key Ks3.

In primarily edited data M11, M12, M13 ... edited by primary users 13, the secondary copyright of primary users 13 is present in addition to the primary copyright of the original data M0 on information providers before being edited. For the purpose of practice this secondary copyright, primary users 13 send the title of data, name of application program, outlined content and the name of primary copyright owner together with third secret-key Ks3 to key control center 12, which are to be stored andd managed by key control center 12.

On the other hand, primary users 13 provide encrypted primarily edited data Cm11ks3, Cm12ks3 and Cm13ks3 ... for secondary users 19 through copying these data into external record medium 18 or by transferring them via network 14.

The secondary users 19 who require to use provided encrypted primarily edited data Cm11ks3, Cm12ks3 and Cm13ks3 ... request key control center 12 for distributing third use permit key K3 including third secret-key Ks3. The usage of primarily edited data M11, M12 and M13 ... by this use permit key K3 is limited to general use succh as display and print and the storing into the storage inside the users terminals. It is not allowed to copy primarily edited data M11, M12 and M13 ... or encrypted primarily edited data Cm11ks3, Cm12ks3 and Cm13ks3 ... into external record medium 18, to transfer these to tertiary users via network 14 and to repeat editing primarily edited data M11, M12 and M13 ....

As described above, the objective of the copyrighted data in this invention is the "object" where the programs and data are integrated. The object can be processed as parts-like through computer programming or various types of processing.

Producing new editorial data using plural original data that are the objects, will be described referring to Figures 4 and 3.

The refence numerals 31, 32 and 33 in FIG. 4 are the original data M31, M32 and M33 that comprise each object for which copyright is claimed. Primarily edted data M30, 30 is produced using these original data M31, M32 and M33.

The number of editorial forms applicable to original data M31, M32 and M33 are three. The first is the primary editorial data M34 shown in 34 where the whole portion is used. The second is the primary editorial form M35 shown in 35 where a part is used. The third is the primary editorial data M36 shown in 36 where the data is used after revision.

Original data is edited by linking copyrighted data by object-unit, referring, embedding and combining it. It is possible to embed and combine copyrighted data freely.

It is also possible to add other matters on the primarily edited data M37, 37 that have been thus combined and embedded in this way.

The primarily edited data M30, 30 newly produced in this way consists of object assembly.

As described above, in the primarily edited data M30 produced in this way, the secondary copyright of primary users 13 in the edition newly arises in addition to the copyright of original data M31, M32 and M33.

For practice this secondary copyright of primary users 13, it is necessary to encrypt primary editorial data. For this purpose, primary users 13 prepare third secret-keys Ks34, Ks35 and Ks36 corresponding to each of primary editorial data M34, M35 and M36, encrypt plaintext primary editorial data M34, M35 and M36 using third secret-keys Ks34, Ks35 and Ks36

$$Cm34ks34 = E\ (Ks34,\ M34)$$

$$Cm35ks35 = E\ (Ks35,\ M35)$$

Cm36ks36 = E (Ks36, M36),
and provide them for secondary users 19 by copying into external record medium 18 or by transferring via network 14.

In addition, primary users 13 register third secret-keys Ks34, Ks35 and s36 to key control center 12. By registering these third secret-keys, the secondary copyright of primary users 13 is registered into key control center 12.

Those sent from primary users 13 to key control center 12 at this time are a plurality of third secret-keys Ks34, Ks35 and Ks36 of which number corressponds to thee number of produced plural primary editorial data, and also the number of third secret-keys, second secret-keys Ks24, Ks25 and Ks26, original data name, information concerning other linking original data, access path to original data used, application programs used for original data M11, M12 and M13 and outlined explanation of copyright works.

Key control center 12 that has received a plurality of third secret-keys Ks34, Ks35 and Ks36 prepares copyright labels Lc34, Lc35 and Lc36 corresponding toa plurality of primary editorial data using original data name, information concerning other linking original data, access path to original data used, application programs used for original data M11, M12 and M13 and outlined explanation of copyright works.

At this time, the linkage between newly produced primary editorial data M34, M35 and M36 and original data M11, M12 and M13 is released. At the time the linkage is released, the entity of the original data that has had so far only relationship as the linkage with primary editorial data M34, M35 and M36 is thus embedded into newly produced primary editorial data M34, M35 and M36. By this, it becomes possible to practice the secondary copyright of encrypted primary editorial data Cm34ks34, Cm35ks35 and Cm36ks36 provided for secondary users 19.

The secondary users 19 who require to use provided encrypted primary editorial data, for example, M34 request key control center 12 for distributing third secret-key Ks34.

Key control center 12 that has received the request for distributing third secret-key Ks 34 distributes the third secret-key Ks34 to secondary users 19 through network 14.

The secondary users 19 who have received third secret-keys Ks3 decrypt encrypted primary editorial data Cm34ks34
M34 = E (Ks34, Cm34ks34)
and use it.

Original data copyright owner or primary editorial data owner can change the access path by applying to key control center 12.

Original data copyright owner or primary editorial data owner can also edit (revise) data using other keys as well as to use third secret-keys.

Claims

1. A data copyright management system used for producing new data by editing a plurality of encrypted data, wherein

a first user obtains a plurality of encrypted data from a database and decrypts said data by using a crypt key supplied from said database;

new data is produced by editing said data decrypted;

said first user supplies both a crypt key for each of said plurality of encrypted data and edition program with digital signature as a use permit key to a second user;

said second user who receives the edited and encrypted data request use of said data by presenting the edition program with digital signature to a copyright management center; and

said copyright management center identifies the first user as an editor with the digital signature, and provides said second user with the crypt key for use when the editor is confirmed bing the first user.

2. A data copyright management system comprising a database and a key control center, and for managing copyrights when a primary user edits primary copyrighted data which is obtained, and supplies secondary copyrighted data obtained through editing to a secondary user, wherein

said primary copyrighted data is encrypted by using a first use permit key and then supplied to said primary user;

said key control center distributes said use permit key to said primary user when said primary user wishing to use said primary copyrighted data requests distribution of said first use permit key to said key control center;

said primary user decrypts said primary copyrighted data for primary use by using said distributed first use permit key;

said primary user wishing to edit said primary copyrighted data is distributed with a second use permit key for editing said primary copyrighted data from said key control center, and edits said primary copyrighted data by using said distributed second use permit key, said copyrighted data during editing being encrypted and stored by using said second use permit key;

said primary user who completes editing is distributed from said key control center with a third use permit key for distributing the edited data, and supplies said edited data to a secondary user after encrypting said edited data by using said third use permit key; and

said secondary user wishing to use said secondary copyrighted data is distributed with said third use permit key from said key control center, and decrypts said secondary copyrighted data by using said distributed third use permit key for use.

3. The data copyright management system according to claim 1, wherein editing of said primary copyrighted data by said primary user is performed on a copy of said primary copyrighted data.

FIG. 1

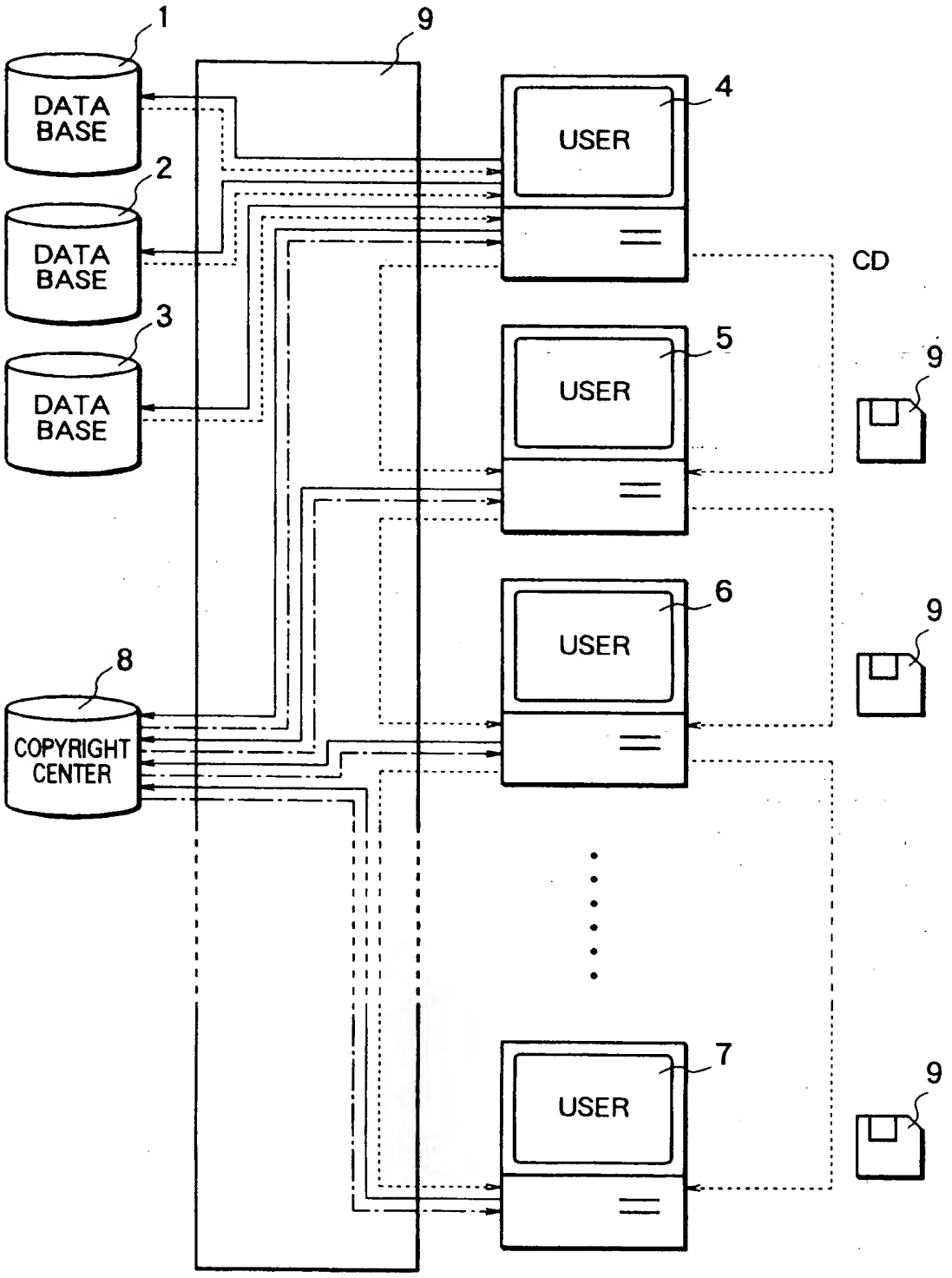


FIG. 2

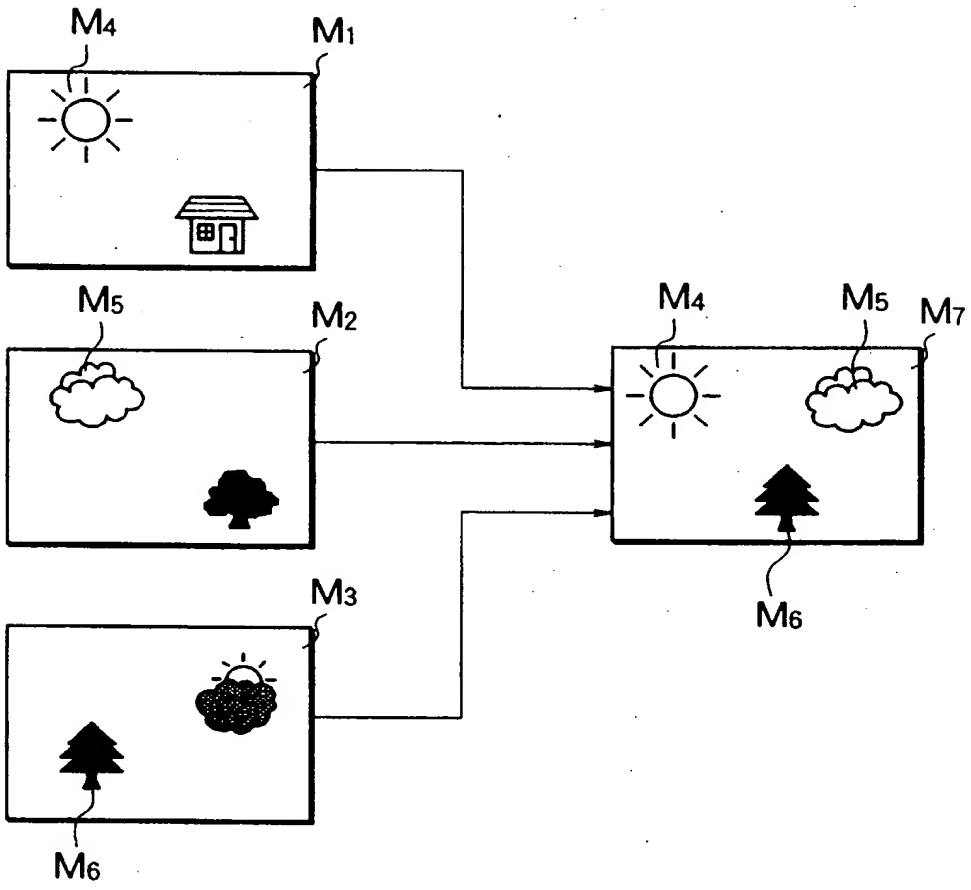


FIG. 3

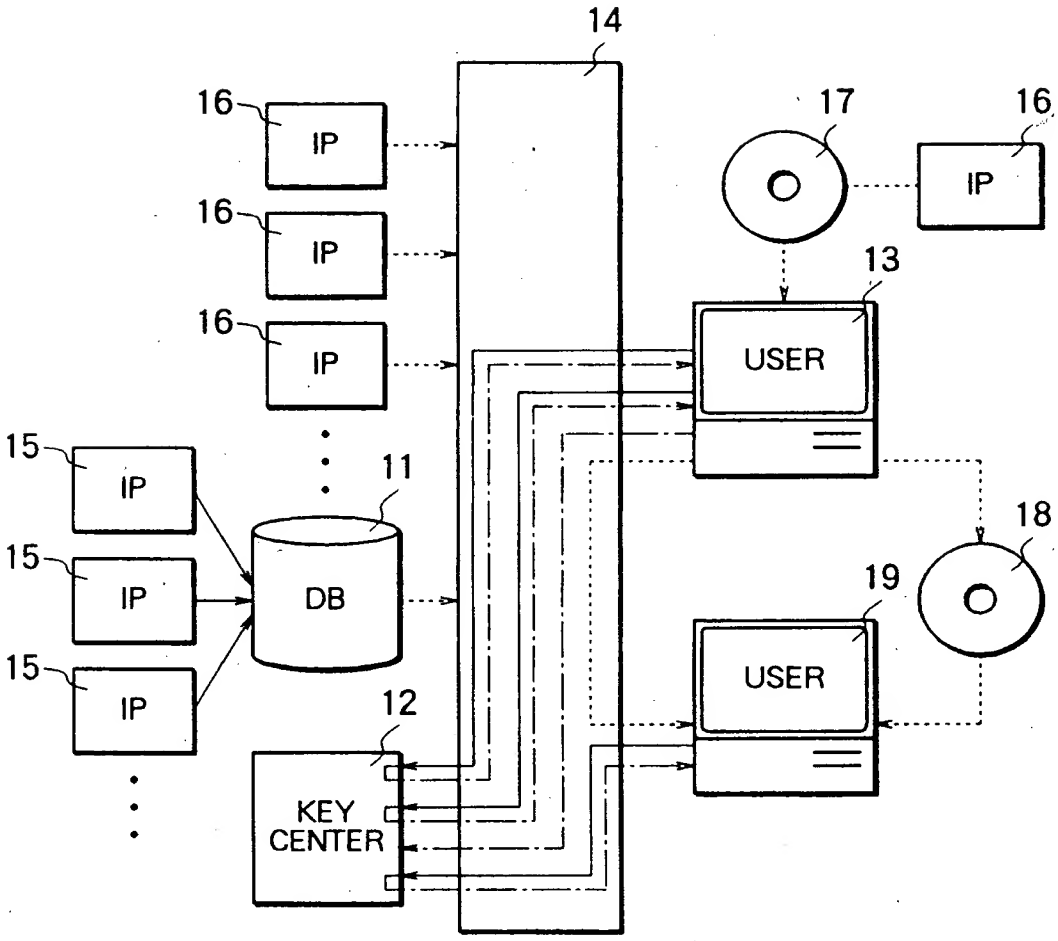
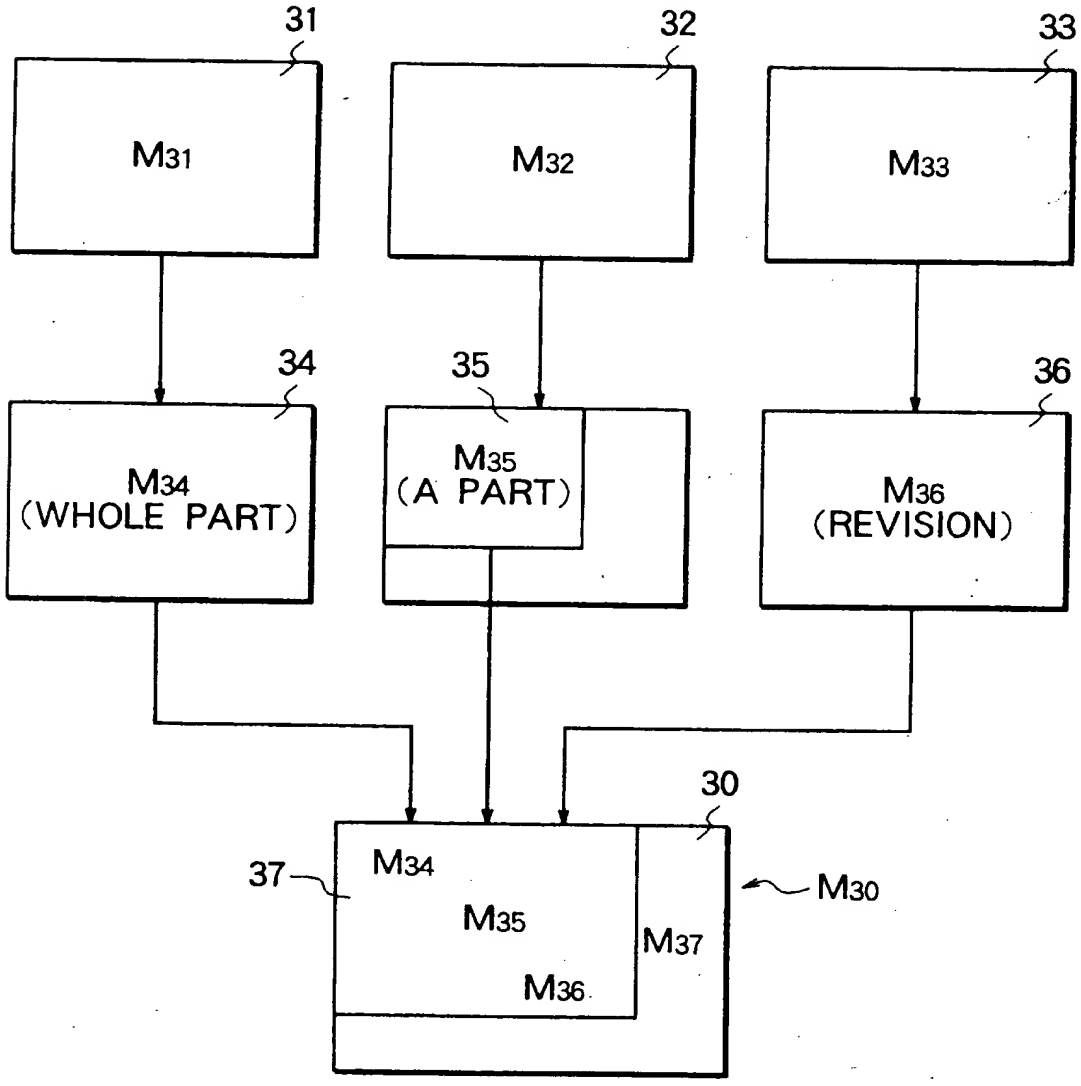


FIG. 4



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 709 760 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
03.02.1999 Bulletin 1999/05

(43) Date of publication A2:
01.05.1996 Bulletin 1996/18

(21) Application number: **95116820.2**

(22) Date of filing: **25.10.1995**

(51) Int. Cl.[6]: **G06F 1/00**, G06F 12/14

(84) Designated Contracting States:
DE FR GB

(30) Priority: **27.10.1994 JP 264201/94**

(71) Applicant:
MITSUBISHI CORPORATION
Chiyoda-ku Tokyo 100 (JP)

(72) Inventors:
- **Saito, Makoto**
  Tokyo (JP)
- **Momiki, Shunichi**
  Tokyo (JP)

(74) Representative:
Neidl-Stippler & Partner
Rauchstrasse 2
81679 München (DE)

(54) Data copyright management system

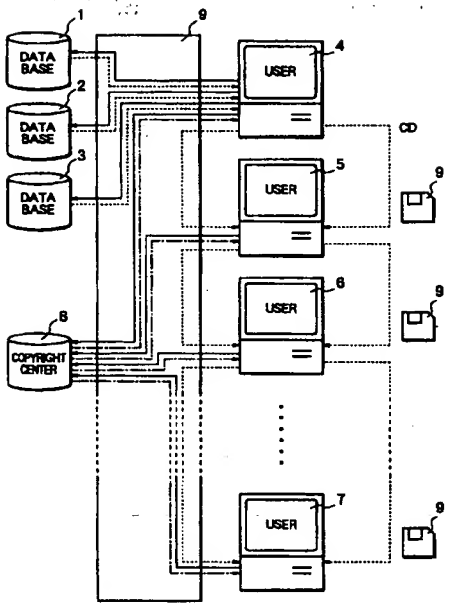
(57) A system is provided which manages the copyright of a plurality of data in a database. A data copyright management system is provided in which a primary user edits data which he or she obtains and supplies edited data to a secondary user.

In a case where new data is produced by editing a plurality of encrypted data obtained from the database, and is encrypted for distribution to another person, crypt keys for a plurality of data as raw material and an edition program which is an editing process with a digital signature are used as a use permit key. When a user who receives the edited and encrypted data requests use of the data by presenting the digital signature to a copyright management center, the copyright management center identifies the editor by the digital signature, and provides the user requiring use of data with the crypt key for use only when the editor is identified to be the valid user of the edited data. The system comprises a database and a key control center, and uses a primary copyright label, a first use permit key including a first crypt key, a second use permit key, a third crypt key, and a copyright management program. The primary user uses primary copyrighted data encrypted by using the first crypt key and supplied, by decrypting it with the first use permit key obtained from the key control center. The data is encrypted again by using the first use permit key when it is stored. The primary user edits the primary copyrighted data by obtaining a second use permit key from the key control center for editing the primary copyrighted data. The data being edited is encrypted and stored by using the second use permit key. At the completion of the editing, the primary user receives the third crypt key for secondary copyright as secondary exploitation right, encrypts the edited data with the third crypt key, and distributes it to a secondary user. The secondary user obtains the third crypt key and uses the edited data.

In another system, in a case where a new data is produced by editing a plurality of data obtained from the database, and encrypted for distribution to another person, crypt keys for a plurality of data as raw material and an edition program which is as an editing process with a digital signature are used as a use permit key. When a user who receives the edited and encrypted data requests use of the data by presenting the digital signature to a copyright management center, the copyright management center identifies the editor by the digital signature, and provides the user requiring data use with a crypt key for use only when the editor is identified to be the valid user of the edited data.

EP 0 709 760 A3

FIG. 1



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 11 6820

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
E	EP 0 704 785 A (MITSUBISHI CORP) 3 April 1996 * abstract; figure 1 * * column 6, line 34 - column 10, line 30 * * column 14, line 30 - column 19, line 52 * * claims 1-3,6,7,23 * ---	1-3	G06F1/00 G06F12/14
A	LEIN HARN ET AL: "A SOFTWARE AUTHENTICATION SYSTEM FOR INFORMATION INTEGRITY" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 11, no. 8, 1 December 1992, pages 747-752, XP000332279 * page 748, right-hand column, line 3 - page 750, right-hand column, line 3 * ---	1-3	
A	US 5 291 598 A (GRUNDY GREGORY) 1 March 1994 * the whole document * -----	1-3	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 December 1998	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 95 11 6820

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-12-1998

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0704785 A	03-04-1996	JP 8185448 A	16-07-1996
US 5291598 A	01-03-1994	US 5375240 A	20-12-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82